OCSP Monitor

Continuous Monitoring and Reporting

ADSS Server is a well-proven, standards-based product that can be deployed on premise for enterprise use or within a managed service as part of a cloud service. It can meet the most demanding needs by providing high throughput and high availability. As a strategic product for Ascertia, it offers support for the latest Windows and Linux operating systems, databases and HSMs.

Certificate Revocation List Overview

Certificate Revocation Lists (CRLs) contain vital information on the revocation status of digital certificates and as such the availability of valid CRLs is essential for normal operation of trust infrastructures. CRLs also form the legal basis for checking the validity and trustworthiness of issued certificates and therefore directly impact the liability model of a PKI system. However, CRL's in large distributed deployments do not provide scale or performance.

OCSP provides end entities a far more scalable and efficient means for end entities to check to see if a digital identity is still trusted. With OCSP, and end entity makes a request to an OCSP Server to check the validity of a certificate. This request checks the specific certificate serial number with a trusted Certificate Authority and an OCSP response is sent back with a response of either 'good', 'revoked' or 'unknown'. In this approach the end entity constructs a simple efficient OCSP query and in milliseconds receives a response instead of having to download and process potentially large CRL files (tens of seconds).

Online Certificate Status Protocol (OCSP) servers are the cornerstone of a trusted PKI infrastructure, providing essential e-ID validation services and are the basis for checking the trust and managing the liability associated with this. It is crucial that their validation policy is checked, that they remain highly available to relying parties and that reliable performance statistics can be provided to check service provider SLAs.

OCSP Monitor allows a variety of positive and negative test cases to be defined. One or more test cases can be defined to run each day within a number of Test Scenarios. Various reports are available to provide summary and detailed results.

Key Features

- **Active monitoring:**
  Automatically and continuously monitors one or more OCSP services for correct functioning and correct results, plus availability and performance
- **Standards Compliant:**
  OCSP Monitor is an RFC 6960 compliant OCSP client and can communicate with RFC 6960 compliant responders
- **Compliance Checking:**
  OCSP responder compliance can be checked using multiple test cases to check compliance with expected validation policy settings

  OCSP Responder availability can be checked using frequent simple test cases to that responses are received in a time way that matches the desired SLA
- **Notification and Reporting:**
  Select which members of staff receive error and summary reports by email and/or phone SMS

  For all test cases OCSP Monitor will record any failures and report on these as well as gather statistics to be detailed in an end of day report. Live reporting is also available – see below
- **Publication and Retention**
  Be able to download CRLs and publish them locally to avoid single point failures and reduce network bandwidth for large enterprises
  Retain a secure and searchable archive of all CRLs that were retrieved, for management information and dispute resolution purposes)

Automated OCSP monitoring

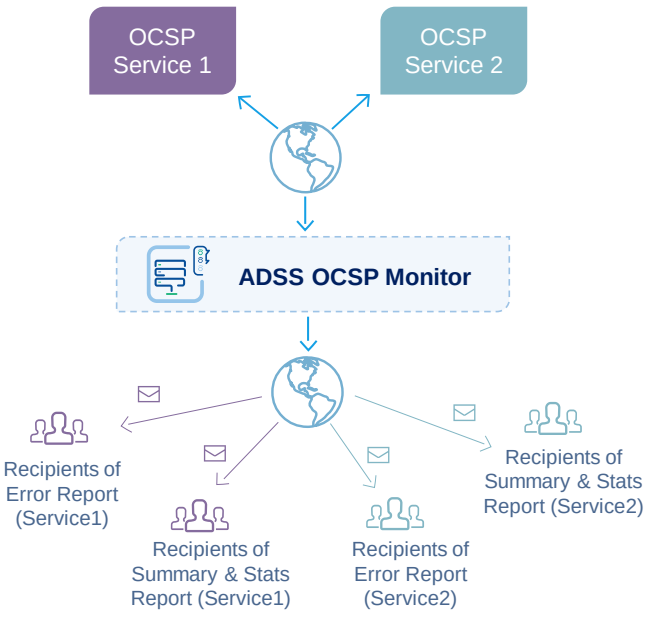
Ascertia OCSP Monitor is a sophisticated test product that enables security administrators to easily detect OCSP service failures or irregularities. It is designed for 24 x 7 automated monitoring although it can also be used interactively when required. OCSP Monitor enables administrators to identify availability or security policy issues and fix unexpected conditions before users report them.

OCSP Monitor is also very useful for organisations that consume OCSP services. They can monitor the service and easily compare this with the Service Level Agreement (SLA). An end-of-day report provides all the key statistics required.

Maximise your OCSP Service uptime

OCSP Monitor provides immediate real-time feedback on OCSP validation issues as they arise. Where OCSP services are used it is often assumed that they are functioning correctly and will continue to do so - this is often not the case.

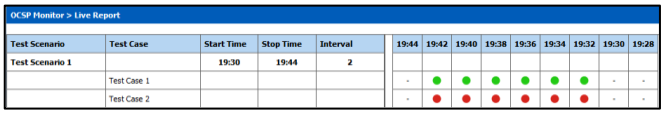
OCSP Monitor allows multiple test scenarios to be run. These can check for expected and unexpected behaviours and monitor OCSP server performance.



Reat-time tests

OCSP Monitor tests the status of your OCSP Servers by making real OCSP client requests. It is easy to set up and manage. Multiple test cases can be defined, and then brought together into one or more test scenarios which run for defined periods each day. These can be quickly amended or added to as required.

The following screen shows the live report dashboard screen that allows administrators to review the results obtained from one or more test scenarios. Green means the test ran as expected and red means the test found a problem. Click on the dots to see the details.



Continuous Monitoring

OCSP Monitor is designed to run 24x7 and allow various Test Scenarios to be run at their configured daily time intervals to monitor performance and validation policy. These approaches are recommended:

- Checking availability and response times by running a check on a valid certificate every few minutes and obtaining the overall service minimum, maximum and average response times
- Checking that a fresh CRL is being used by the OCSP responder, for example using a CRL freshness policy test as required
- Running a comprehensive policy check twice a day to ensure that the defined validation policy is being enforced
- Running checks on disaster recovery systems to ensure they are operational

Detailed Monitoring Checks and Alerts

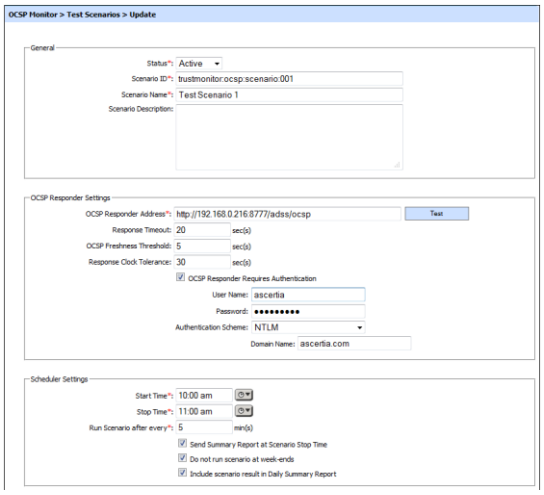
OCSP Monitor has been designed by security experts to provide high quality management information, for example:

- Each test scenario can have several test cases to perform multiple positive and negative checks
- Each test scenario can have its own trust anchors defined for accurate trust checking
- When a test scenario fails a customisable failure report is sent to a defined list of operations
- Customisable reports can be sent using SMS or email or both as required.
- showing the minimum, average and maximum response delay statistics observed as well as a summary of the successful and failed tests observed during the period
- At the end of day a summary report for all scenarios can be sent to service management staff detailing the main statistics for all

Easy Configuration

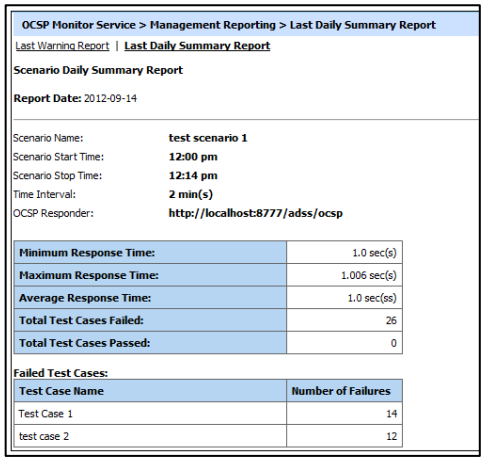
OCSP Monitor has an intuitive wizard to help set-up test scenarios and the required test cases within these. Each test scenario can be set to run between specific start and stop times. Reports can be customised per test scenario.

Part of the Test Scenario update screen is shown below:



Detailed Reporting

OCSP Service Level Agreements can now be accurately checked and reported on. The ability to identify and report on OCSP service issues has been difficult until now. OCSP Monitor provides for easy change of test policies so that a selected level of detailed testing can be carried as required to suit the business demands. History data is maintained and detailed analysis of OCSP request and response data is available as a standard feature. Immediate warning reports and also daily summary reports are produced that provide valuable information:



OCSP Monitor Service > Management Reporting > Last Daily Summary Report

Last Warning Report | **Last Daily Summary Report**

Scenario Daily Summary Report

Report Date: 2012-09-14

Scenario Name: **test scenario 1**
Scenario Start Time: **12:00 pm**
Scenario Stop Time: **12:14 pm**
Time Interval: **2 min(s)**
OCSP Responder: **http://localhost:8777/adss/ocsp**

Minimum Response Time:	1.0 sec(s)
Maximum Response Time:	1.006 sec(s)
Average Response Time:	1.0 sec(ss)
Total Test Cases Failed:	26
Total Test Cases Passed:	0

Failed Test Cases:

Test Case Name	Number of Failures
Test Case 1	14
test case 2	12

OCSP Monitor is a comprehensive solution for actively checking the availability of Certificate Revocation Lists in complex high trust environments.

Secure web-based management is provided as standard together with advanced management configuration options and detailed reporting.

Supported Operating Systems:

Microsoft Server 2022, 2019, 2016
Linux RedHat, SUSE, CentOS, Ubuntu

Supported Databases:

Microsoft SQL Server 2022, 2019, 2017
Oracle 19c, 18c
Azure SQL Database (DB-as-a-service)
PostgreSQL 14, 13, 12, 11
MySQL 8, 5
Percona-XtraDB-Cluster 8, 5

Mike Hathaway | Chief Product Officer

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia's PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

For more info
info@ascertia.com
www.ascertia.com